Amendments to the Claims

1. (Currently amended) A method for transmitting data over a wireless link to a gateway providing access to a wide area network, the method comprising:

encrypting a payload according to a first encryption algorithm;

adding a header to the encrypted payload to form a data packet;

encrypting the encrypted payload and the header of the data packet according to a second encryption algorithm, the second encryption algorithm being an encryption algorithm used for secured communications over the wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network; and

transmitting the encrypted data packet over the wireless link to the gateway.

2. (Previously presented) The method of claim 1, wherein the first algorithm uses a symmetric key.

3. (Previously presented) The method of claim 1, further comprising:

receiving the data packet at the gateway;

decrypting data packet at the gateway according to the second algorithm;

forwarding the recovered data packet to a computer on the wide area network; and

decrypting the payload at the computer on the wide area network according to the

first algorithm.

4. (Previously presented) The method of claim 1, wherein the first algorithm uses a symmetric session key.

5. (Canceled).

6. (Previously presented) A device for transmitting data over a wireless link to a gateway providing access to a wide area network, comprising:

a wireless transceiver; and

an encryption engine coupled to the wireless transceiver for encrypting a payload according to a first encryption algorithm, adding a header to the payload to form a data packet, and encrypting the data packet according to a second encryption algorithm, the second encryption algorithm being an algorithm for secured communications over the wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network.

7. (Canceled).

8. (Previously presented) The device of claim 6, wherein the payload comprises location information regarding the location of the wireless device.

9. (Previously presented) The device of claim 6, wherein the first encryption algorithm employs a symmetric key.

10. (Currently amended) A method for secured communication between a mobile device and a server on a wide area network, comprising:

generating a symmetric session key at the mobile device;

encrypting the symmetric session key at the mobile device using a public key associated with the server;

transmitting the encrypted session key to the server over a wireless link with a gateway to the wide area network;

decrypting the encrypted session key at the server using a private key corresponding to the public key;

encrypting a payload using the symmetric session key at the mobile device;

adding a header to the payload to form a data packet at the mobile device;

encrypting the encrypted payload and the header of the data packet using an encryption algorithm for secured communications over the wireless link to form an encrypted data packet at the mobile device, the encryption data packet being so provided such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network; and

transmitting the encrypted data packet from the mobile device to the gateway.

11. (Previously presented) The method of claim 10, further comprising:

receiving the encrypted data packet at the gateway;

decrypting the encrypted data packet at the gateway to recover a decrypted data packet, the decrypted data packet having the encrypted payload encrypted with

the symmetric session key;

forwarding the decrypted data packet to the server over the wide area network;

decrypting the payload at the server using the decrypted session key.

12-14. (Canceled).

15. (Original) The method of claim 10, wherein the payload includes location information.

16. (Previously presented) The method of claim 10, wherein the generating a symmetric session key at the mobile device further comprises generating the symmetric session key based on a random number.

17. (Original) The method of claim 10, wherein the encrypting a payload using the symmetric session key employs at least one of the encryption algorithms DESX or DES.

18-19. (Canceled).

20. (Previously presented) The method of claim 1, wherein the first algorithm comprises at least one of the encryption algorithms DESX or DES.

21-24. (Canceled).

25. (Previously presented) The method of claim 1, wherein the data packet includes location information.

26. (Previously presented) The method of claim 4, wherein the symmetric session key is generated based on a random number.

27. (Previously presented) The device of Claim 6, further comprising a memory coupled to the encryption engine, the memory having a public key associated with a server on the wide area network stored therein.

28. (Canceled).

29. (Currently amended) A computer readable medium, comprising program instructions for performing a method comprising:

encrypting a payload according to a first encryption algorithm;

adding a header to the encrypted payload to form a data packet;

encrypting the encrypted payload and the header of the data packet according to a second encryption algorithm, the second encryption algorithm being an encryption algorithm used for secured communications over a wireless link, such that the data packet is decrypted according to the second encryption algorithm at the other end of the wireless link and prior to the gateway forwarding the data packet to the wide area network; and

transmitting the data packet to a server on a wide area network over a wireless link with a gateway providing access to the wide area network.

30. (Previously presented) The computer readable medium of claim 29, wherein the first algorithm uses a symmetric key.

31. (Previously presented) The computer readable medium of claim 29, the method further comprising:

receiving the data packet at the gateway;

decrypting data packet at the gateway according to the second algorithm;

forwarding the recovered data packet to a computer on the wide area network; and

decrypting the payload at the computer on the wide area network according to the first algorithm.

32. (Previously presented) The computer readable medium of claim 29, wherein the first algorithm uses a symmetric session key.

33. (Previously presented) The computer readable medium of claim 29, wherein the first algorithm comprises at least one of the encryption algorithms DESX or DES.

34. (Previously presented) The computer readable medium of claim 29, wherein the data packet includes location information.

35. (Previously presented) The computer readable medium of claim 32, wherein the symmetric session key is generated based on a random number.